

RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication :
(A n'utiliser que pour les
commandes de reproduction).

2 486 717

A1

**DEMANDE
DE BREVET D'INVENTION**

(21)

N° 80 15202

(54) Dispositif de transistor pour circuit intégré.

(51) Classification internationale (Int. Cl. 3). H 01 L 29/78, 27/04; H 03 K 13/00, 19/094.

(22) Date de dépôt..... 8 juillet 1980.

(33) (32) (31) Priorité revendiquée :

(41) Date de la mise à la disposition du
public de la demande..... B.O.P.I. — « Listes » n° 2 du 15-1-1982.

(71) Déposant : Société dite : ELECTRONIQUE MARCEL DASSAULT, résidant en France.

(72) Invention de : Jean-Claude Basset et Alain Meinguss.

(73) Titulaire : *Idem* (71)

(74) Mandataire : André Netter, conseil en brevets d'invention,
40, rue Vignon, 75009 Paris.

2° demande divisionnaire bénéficiant de la date de dépôt du 30 novembre 1979 de la
demande de brevet initiale n° 79 29588 (art. 14 de la loi du 2 janvier 1968 modifiée).

L'invention a pour objet un dispositif de circuit intégré à transistors MOS, utilisable notamment pour le codage.

Un circuit intégré à transistors MOS est constitué par une portion de tranche de silicium sur laquelle on
5 a, par une succession de traitements chimiques et/ou physico-chimiques et/ou purement physiques, créé des transistors MOS ainsi que des liaisons électriques entre lesdits transistors, en faisant appel à des masques, réalisant un circuit comme défini au préalable par un ou des dessins.

10 La constitution du circuit intégré, sa fonction, peuvent, par la suite, être reconstitués par la simple observation microscopique.

Cette possibilité de reconstitution d'un circuit intégré entraîne des inconvénients lorsque ledit circuit
15 est destiné à introduire un codage dans une information qu'on veut tenir confidentielle. C'est le cas, par exemple, de circuits faisant partie d'une carte à circuits électroniques destinée à faciliter les transactions d'ordre bancaire ou commercial. C'est également le cas d'un circuit concernant un message
20 quelconque qu'on souhaite tenir confidentiel.

Le dispositif de circuit à transistors MOS selon l'invention élimine ces inconvénients.

L'invention est basée sur cette remarque que les transformations du silicium à l'échelle atomique, qui amènent certaines parties du silicium à jouer le rôle de drain, d'autres
25 à jouer le rôle de source, d'autres à jouer le rôle de grille, en tant que constituants de transistors, sont indécélables à l'observation, même au microscope électronique.

Un circuit selon l'invention, à transistors MOS, est
30 caractérisé par ce fait que, parmi la multiplicité de transistors MOS qu'il comprend, un certain nombre d'entre eux jouent effectivement le rôle de transistors, tandis que d'autres jouent le rôle d'interrupteurs ou de courts-circuits, de sorte qu'à partir d'un même schéma comprenant une multiplicité de tran-
35 sistors, il est possible de réaliser des types différents de circuit suivant la répartition du rôle des transistors en transistors opératoires, transistors interrupteurs et transistors de courts-circuits.

Dans un dispositif de circuit selon l'invention, les
40 pistes conductrices reliant les transistors ne permettent pas,

par leur observation, de reconstituer le schéma effective-
ment opératoire, étant donné que certaines d'entre elles
relient des transistors jouant un rôle d'interrupteur ou un
rôle de court-circuit, de sorte que le dispositif de cir-
cuit et la ou les fonctions logiques qu'il réalise peuvent
5 être considérées comme véritablement cryptées.

L'invention trouve une utilisation dans la réalisation
de dispositif de registre pour l'introduction d'un polynôme de coda-
ge. Alors que jusqu'ici l'observation des circuits de sortie
10 de cases du registre permet la reconstitution du polynôme,
le dispositif de codage à registre selon l'invention com-
prend un circuit de sortie pour chacune des cases et, dans
le cas d'un registre série, des transistors sur chacun des
circuits de sortie, et c'est la nature des transistors MOS,
15 dépendante du dopage introduit, indécidable à l'observation
qui réalise le montage de codage.

Le procédé de fabrication d'un dispositif de circuit
selon l'invention est, dans l'ensemble, analogue à celui uti-
lisé pour la fabrication d'un circuit intégré à transistors
20 MOS.

Il prévoit cependant l'intervention de moyens permet-
tant le dosage du dopage, soit qu'en certains emplacements
de la tranche de silicium aucun dopage ne soit introduit, et
ainsi aucun transistor formé, ou bien que le dopage soit in-
25 suffisant pour l'obtention d'un transistor opératoire.

Cette sélection peut être obtenue à l'aide de masques.

Elle peut aussi être obtenue par un ajustement du
degré d'action du moyen utilisé pour le dopage, soit par un
réglage du temps d'action, soit par le réglage d'une tension
30 électrique dont dépend la profondeur de l'action, soit par
les dimensions et/ou la disposition d'ouvertures d'un masque,
etc.

La sélection peut s'opérer quel que soit le moyen uti-
lisé pour le dopage : diffusion chimique, bombardement ioni-
35 que, etc.

Dans la description qui suit, faite à titre d'exemple,
on se réfère aux dessins annexés, dans lesquels :

la figure 1 est un schéma d'un dispositif de registre
connu ;

40 la figure 2 est un schéma d'un dispositif de registre;

selon l'invention ;

la figure 3 est un symbole représentatif d'un transistor dans une certaine condition ;

la figure 4 est analogue à la figure 3 mais pour une autre condition du transistor ;

la figure 5 est analogue aux figures 3 et 4 mais pour encore une autre condition du transistor.

Le registre R comprenant dix cases, numérotées de 0 à 9, est propre à introduire un codage polynomial dans une information appliquée à son entrée e. Le montage classique représenté sur la figure 1 correspond au codage par le polynôme ci-après, choisi à titre d'exemple :

$$x_0 + x_5 + x_7 + x_9$$

Dans ce but, la case 9 est reliée par un conducteur C_9 à une porte OU exclusif $P_{7.9}$ dont l'autre entrée est reliée par un conducteur C_7 à la case 7. La sortie de la porte 7.9 est reliée à une première entrée d'une seconde porte $P_{5.7.9}$ dont l'autre entrée est reliée par un conducteur C_5 à la case 5, et la sortie de la porte $P_{5.7.9}$ est reliée à une première entrée d'une porte $P_{0.5.7.9}$ dont l'autre entrée est reliée par un conducteur C_0 à la case 0, l'information codée étant présente à la sortie s du dispositif, chacune des portes P étant constituée par des transistors MOS.

L'observation au microscope électronique de la partie entourée par le rectangle en trait pointillé permet la détermination du polynôme de codage.

Le dispositif selon l'invention assurant le même codage polynomial, mais crypté, est montré schématiquement sur la figure 2. Il comprend le même registre R à dix cases 0, 1, etc., 9, à l'entrée e duquel est appliquée l'information d'entrée à coder. De chacune des cases est issu un conducteur $C_9, C_8 \dots C_0$. Le conducteur C_9 relie électriquement la case 9 à l'entrée 11 d'un circuit à transistors 12 à seconde entrée 13, le circuit 12 ayant des transistors amenés dans un état tel qu'il joue un rôle de court-circuit entre l'une ou l'autre de ses entrées 11 et 13 et sa sortie 14. Un transistor propre à jouer un rôle de court-circuit est sym-

bolisé sur la figure 3.

Sur le conducteur C_8 est interposé un "transistor" dont l'état est tel qu'il joue un rôle d'interrupteur, comme schématisé par le symbole de la figure 4.

5 Sur le conducteur C_7 issu de la case 7 est prévu un "transistor" de court-circuit 16 du type montré sur la figure 3 et la porte OU exclusif 17 est reliée par une de ses entrées 18 au transistor 16 et par son autre entrée 19 à la sortie 14 du circuit 12. Les transistors constitutifs de la
10 porte 17 sont du type habituel, comme rappelé par le symbole de la figure 5.

On trouve réalisé à la sortie 21 de la porte 17 l'ensemble formé par deux des termes du polynôme, à savoir :

$$x_9 + x_7$$

15 La sortie 21 est reliée à la première entrée 22 d'un circuit 23 à transistors en court-circuit et dont l'autre entrée 24 est reliée à la case 6 par l'intermédiaire d'un transistor 25 du type représenté sur la figure 4, c'est-à-dire jouant le rôle d'interrupteur.

20 Sur le conducteur C_5 est interposé un circuit à transistors 26 jouant le rôle de court-circuit, et le circuit OU exclusif 27 comprend des transistors du type habituel. Sur le conducteur C_4 est interposé un transistor-interrupteur et il en est de même sur les conducteurs C_3 , C_2 , C_1 . Sur le
25 conducteur C_0 est par contre interposé un transistor de court-circuit du type montré sur la figure 3.

A la sortie \underline{g} est présente l'information codée par le polynôme

$$x_0 + x_5 + x_7 + x_9$$

30 Le dispositif montré sur la figure 2 assure ainsi le même codage que le dispositif montré sur la figure 1 mais, alors que la disposition des circuits du dispositif selon la figure 1 traduisait le codage introduit entre l'entrée \underline{g} et la sortie \underline{g} , la disposition des circuits sur la figure 2 ne
35 donne aucune information sur le polynôme de codage.

Cette disposition reste la même quel que soit le polynôme introduit pour le codage.

Au moment de la fabrication de la "puce", la sélection entre les transistors qui doivent jouer le rôle habituel de
40 transistors et ceux devant jouer un rôle de court-circuit ou un

rôle d'interrupteur, se fait par l'utilisation de masques supplémentaires au cours d'une phase de dopage, d'où résulte un ajustement de l'action de l'agent de dopage, que celui-ci soit chimique ou physique.

5 La métallisation est la même quel que soit le polynôme à réaliser, ainsi d'ailleurs que la disposition des transistors. Il est donc impossible, par l'observation des circuits de métallisation ou des transistors présents, d'être informé sur le codage introduit par le dispositif.

10 Un tel dispositif de codage crypté trouve une utilisation particulièrement intéressante dans la constitution d'une carte à circuits électroniques utilisable pour des transactions commerciales et/ou financières, en rendant très difficile, sinon impossible, à un fraudeur, la détermination
15 du code utilisé dans l'échange d'informations entre la carte et un terminal.

Le dispositif selon l'invention trouve des applications dans des domaines autres que celui de la carte de crédit ou de la carte d'achat.

REVENDICATIONS

1. Transistor en circuit intégré, caractérisé en ce que le dopage de ses constituants est tel qu'il réalise un court-circuit entre sa source et son drain.
- 5 2. Transistor en circuit intégré, caractérisé en ce que le dopage de ses constituants a été conduit pour qu'il réalise une interruption de courant entre sa source et son drain.
- 10 3. Cellule de réalisation de fonction logique à transistors en circuit intégré et interconnexions entre les transistors, caractérisée en ce que certains des transistors de la cellule sont dopés de manière à réaliser un court-circuit et d'autres dopés de manière à réaliser une interruption.

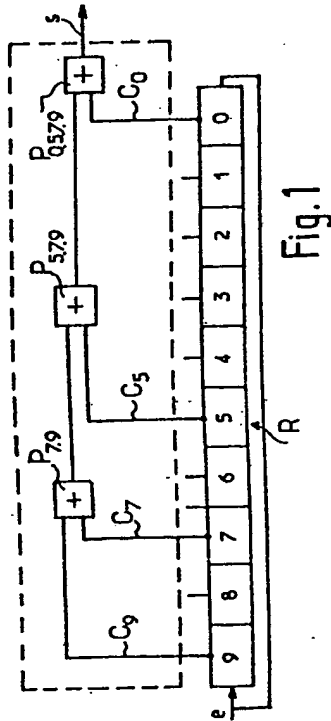


Fig. 1

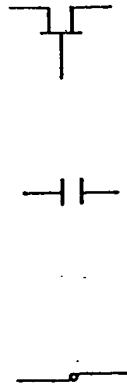


Fig. 3

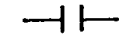


Fig. 4



Fig. 5

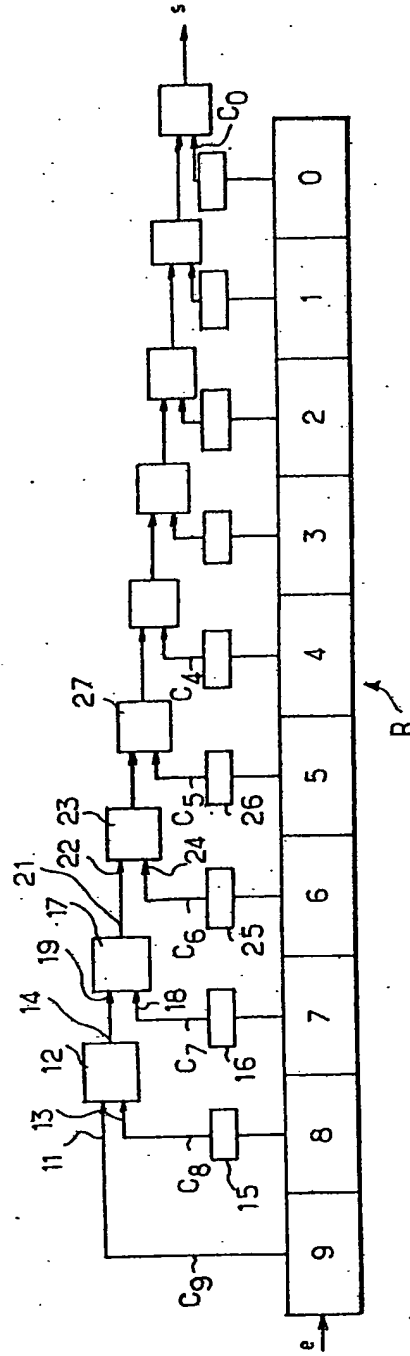


Fig. 2

Handwritten signature